

Service Definition:

Identity and Access Management Services

1. Service Overview

In the modern digital workplace, managing user identities and access rights is critical for both security and operational efficiency. The Bytes Identity & Access Management Service provides a comprehensive solution to manage the full employee lifecycle—Joiners, Movers, and Leavers (JML).

This service automates the complex processes of provisioning and de-provisioning access, ensuring that the right people have the right access at the right time. By integrating robust governance with automated workflows, Bytes help organisations eliminate security risks associated with "permissions creep," reduce the administrative burden on IT teams, and ensure a seamless experience for end-users requesting software licenses or system access.

2. Service Features and Benefits

The following table outlines the core value proposition of the service:

Feature	Benefit
JML Process Automation	Streamlines the lifecycle of employees from onboarding to offboarding, reducing manual effort, and minimising human error.
Single Sign-On (SSO)	Enhances user experience and productivity by allowing access to multiple applications with a single set of credentials.
Multi-Factor Authentication (MFA)	Strengthens security posture by requiring multiple forms of verification, protecting against unauthorised access.
License Assignment & Request Management	Provides a structured, automated workflow for users to request software licenses, ensuring approval governance before automatic assignment.
Privileged Access Management (PAM)	Secures critical assets by monitoring and controlling users with elevated permissions to prevent misuse.
Identity Governance (IGA)	Audits user access rights to ensure compliance with internal policies and external regulations (e.g., ISO27001).

3. Service Scope and Modules

3.1 JML Lifecycle Automation

Bytes can design and implement automated workflows to manage the three critical stages of the employee lifecycle:

- **Joiners (Onboarding):** Automatic account creation and "birthright" access provisioning based on role, department, and location. Ensures new starters are productive from Day 1.
- **Movers (Cross-boarding):** Dynamic adjustment of access rights when an employee changes roles. This includes removing old permissions to prevent "privilege creep" and adding new ones relevant to the new post.
- **Leavers (Offboarding):** Immediate, automated revocation of access across all systems and cloud tenants upon termination, preventing data exfiltration and ensuring license recovery.

3.2 License Request and Assignment Service

To control software spend, and ensure compliance, Bytes can implement a managed request service for software licensing:

Activity	Description
Self-Service Portal	Implementation of a user-facing portal where employees can browse a catalogue of approved software and submit requests.
Approval Workflows	Configuration of multi-stage approval gates (e.g., Line Manager -> Budget Holder -> IT Admin) to validate business need and budget availability.
Automated Provisioning	Once approved, the service triggers automated assignment of the license via API connectors (e.g., to M365, Adobe, or Salesforce), removing manual IT intervention.
Reclamation & Harvesting	Automated identification and removal of unused licenses to return them to the pool for re-assignment.

3.3 Identity Security and Governance

Bytes can secure the identity perimeter through rigorous configuration and ongoing management:

Activity	Description
Tenant Security Optimisation	Continuous assessment of your tenant against security best practices (e.g., Microsoft Secure Score) with remediation planning.
Conditional Access Policies	Implementation of context-aware access rules (e.g., blocking login from high-risk locations or unmanaged devices).
Access Certification Reviews	Scheduled campaigns where managers must review and re-certify their subordinates' access rights to maintain compliance.

4. Onboarding and Implementation

Bytes use a structured onboarding methodology to ensure the service is tailored to your specific organisational hierarchy and security requirements.

Phase	Activity	Description
Discovery	Role Mining & Analysis	Mapping of job roles to required applications (RBAC) and definition of approval hierarchies for license requests.
Design	Workflow Definition	Designing the specific "If This Then That" logic for JML events and license request flows.
Build	Configuration & Integration	Configuring the IDP (Identity Provider), setting up SSO/MFA, and building connectors to HR systems and downstream apps.
Transition	UAT & Training	User Acceptance Testing of workflows and delivery of familiarisation training for service desk and end-users.

5. Service Governance and Support

5.1 Support Model

Activity	Description	Service Hours
Incident Management	Resolution of issues related to authentication failures, failed provisioning jobs, or access errors.	Standard Business Hours
Policy Management	Updates to conditional access policies, approval routing, or role definitions as business needs evolve.	On Request
Audit Support	Provision of access logs and reports to support internal or external compliance audits.	On Request

5.2 Tasks and Responsibilities (RACI)

The following matrix defines the division of responsibilities to ensure clarity in service delivery.

Activity	Bytes	Customer
HR Data Integrity (Source of Truth)		X
Identity Platform Configuration	X	
Approval of Access Requests		X
Workflow Logic Design	X	C
License Procurement	X	X
Device distribution to End Users		X

6. Service Exclusions

The following areas are excluded from the standard managed service scope but may be addressed via separate professional services engagements:

- Custom App Integration: Development of custom API connectors for legacy or unsupported applications is not included in the standard fee.
- HR System Management: Bytes do not manage the HRIS (Human Resource Information System) itself; Bytes do rely on it as a data source.
- Physical Asset Recovery: Collection of physical laptops/devices from leavers is a customer responsibility unless a specific asset disposal service is purchased.
- End User Data Backup: While Bytes secure access, backing up the data created by the user (e.g., on their desktop) is outside the scope of IAM.

7. Commercial Structure

Service Option	Description
Pricing Model	Fixed Cost / per User per Month
Payment Model	Annual or Monthly
Term	Minimum 12 Months